--Cross-Reference to Related Applications
This is a national phase filing of International Application No. PCT/SG2004/000312, which was filed on September 24, 2004, and claims priority of United States Patent Application No. 60/506,315 filed on September 26, 2003.--

SUMMARY

In accordance with a first aspect of the present invention there is provided a method of protecting a digital image, the method comprising extracting feature values from the digital image based on a selected authentication bit-rate~~; embedding~~ **and a selected image content; selecting an authentication mode for processing the extracted feature values, the processing of the extracted feature values comprising deriving** data corresponding to the ~~feature values as a watermark into the digital image~~**extracted feature values based on the selected authentication mode**; and creating an image signature based on the data corresponding to the feature values.

The ~~method~~**processing** may ~~further~~ comprise ~~the step of selecting a desired authentication robustness level, and error~~ correcting coding **(ECC)** the extracted feature values ~~prior~~ to ~~embedding~~**derive** the data corresponding to the feature values~~ into the digital image~~.

The feature values from each of a plurality of codeblocks of the original digital image may be thresholded and coded to create the data corresponding to the feature values.

The ~~coding of the thresholded feature values~~**processing** may **further** comprise ~~ECC coding to generate parity check bits (PCBs) as~~**embedding** the data corresponding to the feature values **into the digital image**.

The method may further comprise applying ECC coding again to ~~the PCBs~~**parity check bits generated during the ECC coding of the extracted feature values** to generate the data corresponding to the feature values**,**

The embedding of the data corresponding to the feature values as a watermark may be conducted in a lossy or a lossless way, based on the selected authentication mode.

The creating of the image signature may comprise applying a cryptographic hashing function to a bit sequence representing the data corresponding to the feature values.

The creating of the image signature may comprise utilising a private key.

The method may further comprise distributing the digital image, including the embedded data, as the authentic digital image.

The method may further comprise coding the digital image, including the embedded data, utilising JPEG2000 compression.

The extracting of the feature values, the embedding of the data corresponding to the feature values, and the creating of the image signature may be performed as part of the JPEG 2000 coding.

In accordance with a second aspect of the present invention there is provided a method of authenticating a digital image, the method comprising extracting ~~data embedded as a watermark in the digital image; extracting~~ feature values from the digital image ~~at~~**based on** a selected authentication bit-rate; **and** processing the extracted ~~data and extracted~~ feature values to derive data corresponding to original feature values **based on a selected authentication mode**; and comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.

~~The deriving of~~**Deriving** the data corresponding to the ~~original~~ feature values may comprise ~~error correcting~~**ECC** coding the extracted data and extracted feature values.

The extracted ~~data and extracted~~ feature values from each of a plurality of codeblocks of the digital image may be decoded to derive the data corresponding to the original feature values.

The ~~extracted data~~**method** may **further** comprise ~~PCBs, and the decoding of the extracted data and~~**extracting data embedded as a watermark in the digital image; and the processing the** extracted **data and the extracted** feature values ~~comprises ECC decoding~~**to derive the data corresponding to original feature values**.

The method may further comprise applying ECC decoding twice to the extracted data.

The data may be embedded in a lossy or lossless way as a watermark in the digital image.

The method may further comprise applying a cryptographic technique to the image signature to derive a bit sequence representing the reference data.

The method may further comprise applying a public key to process the image signature for deriving the reference data.

The method may further comprise receiving the digital image as a coded digital image.

The digital image may be coded utilising JPEG2000.

The extracting of the data embedded as a watermark, the extracting of ~~the~~ feature values from the digital image, the processing of the extracted data and extracted feature values~~ to derive data corresponding to original feature values~~, and the comparing of the derived data corresponding to the original feature values with the reference data may be performed as part of the JPEG 2000 de-coding.

In accordance with a third aspect of the present invention there is provided a system for protecting a digital image, the system comprising a feature value extractor device for extracting feature values from the digital image based on a selected authentication bit-rate; a ~~watermarking device for embedding~~**mode selector for selecting an authentication mode for processing the extracted feature values; a processor device for deriving** data corresponding to the **extracted** feature values ~~as a watermark into the digital image; and a~~**based on the selected authentication mode; and wherein the** processor device ~~for creating~~**further creates** an image signature based on the data corresponding to the feature values.

In accordance with a fourth aspect of the present invention there is provided a computer readable data storage medium having stored thereon computer program code means for instructing a computer to execute a method of protecting a digital image, the method comprising extracting feature values from the digital image based on a selected authentication bit-rate; ~~embedding~~**selecting an authentication mode for processing the extracted feature values, the processing of the extracted feature values comprising deriving** data corresponding to the **extracted** feature values ~~as a watermark into the digital image~~**based on the selected authentication mode**; and creating an image signature based on the data corresponding to the feature values.

In accordance with a fifth aspect of the present invention there is provided a system for authenticating a digital image, the system comprising ~~an extraction device for extracting data embedded as a watermark in the digital image;~~ a feature value extractor device for extracting feature values from the digital image based on a selected authentication bit-rate; a processor device for processing the extracted ~~data and the extracted~~ feature values **based on a selected authentication mode** to derive data corresponding to original feature values and for comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.

In accordance with a sixth aspect of the present invention there is provided a computer readable data storage medium having stored thereon computer program code means for instructing a computer to execute a method of authenticating a digital image, the method comprising extracting ~~data embedded as a watermark in the digital image; extracting~~ feature values from the digital image based on a selected authentication bit-rate; processing the extracted ~~data and extracted~~ feature values **based on a selected authentication mode** to derive data corresponding to original feature values; and comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.